

Optimal strongly conflict-avoiding codes of even length and weight three

Yijin Zhang · Yuan-Hsun Lo ·
Wing Shing Wong

Received: date / Accepted: date

Abstract Strongly conflict-avoiding codes (SCACs) are employed in a slot-asynchronous multiple-access collision channel without feedback to guarantee that each active user can send at least one packet successfully in the worst case within a fixed period of time. By the assumption that all users are assigned distinct codewords, the number of codewords in an SCAC is equal to the number of potential users that can be supported. SCACs have different combinatorial structure compared with conflict-avoiding codes (CACs) due to additional collisions incurred by partially overlapped transmissions. In this paper, we establish upper bounds on the size of SCACs of even length and weight three. Furthermore, it is shown that some optimal CACs can be used to construct optimal SCACs of weight three.

Keywords strongly conflict-avoiding code · conflict-avoiding code · protocol sequence

Mathematics Subject Classification (2010) 94B25 · 94C30 · 11A15

Y. Zhang
School of Electronic and Optical Engineering, Nanjing University of Science and Technology,
Nanjing, China
E-mail: yijin.zhang@gmail.com

Y.-H. Lo
Department of Mathematics, National Taiwan Normal University, Taipei 116, Taiwan
E-mail: yhlo0830@gmail.com

W. S. Wong
Department of Information Engineering, the Chinese University of Hong Kong, Hong Kong
E-mail: wswong@ie.cuhk.edu.hk

1 Introduction

1.1 Motivation

The collision channel without feedback model [8] is investigated in this paper. There are total M potential users and at most k users are active at the same time. *Protocol sequences* [3, 12, 13, 16, 17, 19] are used to provide multiple-access. Let $x_i = (x_{i,0}, x_{i,1}, \dots, x_{i,L-1})$ be a binary protocol sequence with length L assigned to user i . Each active user sends its packet to a common sink if and only if the assigned sequence value equals one. The channel time is partitioned into fixed-length slots and the packet length exactly occupies a slot. A total overlap of packets occurs if more than one user start their transmission simultaneously; and a partial overlap of packets occurs if one packet starts or ends its transmission within the transmission duration of some other packet. Any partial or total overlap of packets would incur a collision. A packet without suffering from any collision is received error-free; otherwise it is assumed to be unrecoverable. As there is no feedback from the receiver and no cooperation among the users, each user has a relative delay offset. Let δ_i be the time offset of user i for $i = 1, 2, \dots, M$, measured in time slot duration units. As introduced in [8], there are two different levels of synchronization:

- (i) The channel is *slot-synchronized* if all users start transmitting at the slot boundaries, i.e., the time offsets $\delta_1, \delta_2, \dots, \delta_M$ are arbitrary integers. Collisions will result only when packets totally overlap.
- (ii) The channel is *slot-asynchronous* if all users do not know the slot boundaries of the channel, i.e., the time offsets $\delta_1, \delta_2, \dots, \delta_M$ are arbitrary real numbers. Some collisions may be incurred by partial overlap of packets.

A set of M binary sequences $\{x_1, x_2, \dots, x_M\}$ is said to be an $(M, k, \omega, L, \sigma)$ *protocol sequence set* [12] if any sequence is of length L , Hamming weight ω , and has the property that each active user can transmit at least σ packets successfully in a period of L slots in the worst case. When $\sigma \geq 1$, we say this sequence set enjoys the *nonblocking property*. Obviously, whether $\sigma \geq 1$ or not highly depends on the assumption of synchronization.

Let \mathcal{I} be a codeword of weight ω over \mathbb{Z}_L . Since a binary sequence of length L can be identified with a subset of \mathbb{Z}_L representing the indices of nonzero positions, a set of M protocol sequences can be viewed as a code consisting of M codewords. In order to provide the nonblocking property at different levels of synchronization, the following two classes of codes have been studied as protocol sequences extensively in the literature.

- (i) An $(M, k, \omega, L, \sigma)$ protocol sequence set is a *conflict-avoiding code* (CAC) [1, 2, 4, 5, 7, 9, 10, 11, 14, 15] if $k = \omega$ and $\sigma = 1$ in the slot-synchronized case.
- (ii) An $(M, k, \omega, L, \sigma)$ protocol sequence set is a *strongly conflict-avoiding code* (SCAC) [20] if $k = \omega$ and $\sigma = 1$ in the slot-asynchronous case. SCACs consider a more practical channel model.

As $k = \omega$, both CACs and SCACs require that there is at most one collision between any two distinct sequences for any relative delay offsets. However,

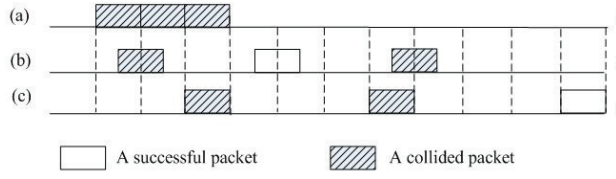


Fig. 1 (a) Packets from user 1, (b) packets from user 2, (c) packets from user 3.

collisions incurred by partially overlapped transmissions need to be additionally considered in the design of SCACs. This yields different combinatorial structures of CACs and SCACs, as argued in [20]. Before presenting them accordingly in Section 2, we provide an example first as the following.

$$\begin{aligned} x_1 &= (1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \\ x_2 &= (1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0) \\ x_3 &= (1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0) \end{aligned}$$

$\{x_1, x_2, x_3\}$ forms a CAC with $M = 3$ and $L = 12$. However, it is not an SCAC. For $\delta_1 = 1$, $\delta_2 = 1.5$ and $\delta_3 = 3$, all packets from user 1 are lost due to two partial overlappings and one complete overlapping, as illustrated in Fig. 1.

In the study of CAC or SCAC, the main theme is to find as many sequences (or, codewords) as possible, for a given pair of integers L and w . If a CAC or SCAC enjoys the maximal size of codewords, then this code is said to be *optimal*.

Asymptotically optimal and optimal CACs for general weights were investigated in [14, 15]. Based on previously known constructions of CACs, asymptotically optimal SCACs are derived in [20] under the assumption that each codeword possesses a special structure, called equi-difference. Moreover, optimal CACs of weight three are investigated in [1, 2, 4, 5, 7, 9, 11]. The code size spectrum of optimal CACs with even length and weight three has been completely settled by these studies. However, relatively little is known about the code size of optimal SCACs. In this paper, we are going to find optimal SCACs of even length and weight three, which can be applied to more realistic scenarios.

The rest of this paper is organized as follows. In Section 2, we introduce some relevant definitions and relative known results in the literatures, as well as present a necessary condition for the existence of an SCAC. Several useful properties of codewords in an SCAC are given in Section 3. New upper bounds on the size of SCACs are derived in Section 4. In Section 5 we prove that some upper bounds in Section 4 are indeed tight in several cases. Finally, conclusions are given in Section 6.

2 Preliminaries

2.1 Definitions and notations

Let $\mathbb{Z}_L = \{0, 1, \dots, L-1\}$ denote the ring of residues modulo L and $\mathcal{P}(L, \omega)$ denote the set of all ω -subsets of \mathbb{Z}_L . Each element $x \in \mathcal{P}(L, \omega)$ can be identified with a binary sequence of length L and weight ω representing the indices of the nonzero positions. Therefore, a CAC or SCAC of length L and weight ω can be viewed as a subset of $\mathcal{P}(L, \omega)$. We call elements in $\mathcal{P}(L, \omega)$ *codewords*.

For a codeword $\mathcal{I} \in \mathcal{P}(L, \omega)$, let $d(\mathcal{I}) := \{a - b \pmod{L} : a, b \in \mathcal{I}\}$ denote the *set of differences* between pairs of elements in \mathcal{I} , and let $d^*(\mathcal{I}) := d(\mathcal{I}) \setminus \{0\}$ denote the *set of non-zero differences* in \mathcal{I} . Then a formal definition of a CAC can be given as follows.

Definition 1 A CAC of length L and weight ω is a subset $\mathcal{C} = \{\mathcal{I}_1, \dots, \mathcal{I}_M\} \subset \mathcal{P}(L, \omega)$ satisfying the condition that for all $j \neq k$,

$$d^*(\mathcal{I}_j) \cap d^*(\mathcal{I}_k) = \emptyset. \quad (1)$$

For given L and w , let $\text{CAC}(L, \omega)$ denote the class of all CACs of length L and weight w . The maximum size of a code in $\text{CAC}(L, \omega)$ is denoted by $M(L, \omega)$. A code $\mathcal{C} \in \text{CAC}(L, \omega)$ is said to be *optimal* if $|\mathcal{C}| = M(L, \omega)$.

Given two subsets $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_L$, let $\mathcal{A} \pm \mathcal{B} := \{a \pm b \pmod{L} : a \in \mathcal{A}, b \in \mathcal{B}\}$. Then an SCAC can also be defined by means of d and d^* .

Definition 2 An SCAC of length L and weight ω is a subset $\mathcal{C} = \{\mathcal{I}_1, \dots, \mathcal{I}_M\} \subset \mathcal{P}(L, \omega)$ satisfying the condition that for all $j \neq k$,

$$\left(d^*(\mathcal{I}_j) \cup (d^*(\mathcal{I}_j) + \{1\}) \cup (d^*(\mathcal{I}_j) - \{1\}) \right) \cap d(\mathcal{I}_k) = \emptyset. \quad (2)$$

This definition captures all the possibilities of partial collisions in slot asynchronous systems.

Similarly, for given L and w , let $\text{SCAC}(L, \omega)$ denote the class of all SCACs of length L and weight w . The maximum size of a code in $\text{SCAC}(L, \omega)$ is denoted by $M_S(L, \omega)$. A code $\mathcal{C} \in \text{SCAC}(L, \omega)$ is said to be *optimal* if $|\mathcal{C}| = M_S(L, \omega)$.

Given a code \mathcal{C} in $\text{CAC}(L, \omega)$ or $\text{SCAC}(L, \omega)$, a codeword $\mathcal{I} \in \mathcal{C}$ is called *equi-difference* if all its elements form an arithmetic progression in \mathbb{Z}_L , i.e., $\mathcal{I} = \{0, g, 2g, \dots, (\omega-1)g\}$ for some $g \in \mathbb{Z}_L$, where the product fg is calculated modulo L . The element g is called the *generator* of \mathcal{I} . Without loss of generalization, we assume $g \leq L/2$ in this paper. A code is called *equi-difference* if it entirely consists of equi-difference codewords. We use $M^e(L, \omega)$ (or $M_S^e(L, \omega)$) to denote the maximum code size among all equi-difference CACs (or SCACs) of length L and weight w .

For a codeword $\mathcal{I} \in \mathcal{P}(L, \omega)$ define the *set of shifted non-zero differences* of \mathcal{I} by $d^+(\mathcal{I}) := d^*(\mathcal{I}) + \{0, 1\}$. Then the definition of an SCAC can be rewritten as follows.

Proposition 1 ([20]) $\mathcal{C} = \{\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_M\} \in \text{SCAC}(L, \omega)$ if and only if

- (i) $\{1, L-1\} \cap d^*(\mathcal{I}_j) = \emptyset$ for all j ; and
- (ii) $d^+(\mathcal{I}_j) \cap d^+(\mathcal{I}_k) = \emptyset$ for all $j \neq k$.

Proposition 1 implies directly that for any $\mathcal{C} \in \text{SCAC}(L, \omega)$, the following holds:

$$\bigcup_{\mathcal{I} \in \mathcal{C}} d^+(\mathcal{I}) \subseteq \{2, 3, \dots, L-1\}. \quad (3)$$

Let \mathcal{A} be a subset of \mathbb{Z}_L . A subset of \mathcal{A} which consists of consecutive integers is called a closed interval. A closed interval S is maximal if for any other closed interval T , either $T \subset S$ or $T \cap S = \emptyset$. Obviously, \mathcal{A} can be uniquely partitioned into several maximal closed intervals, called *tubes*. A tube is denoted by $T(x, y)$ if its smallest and largest integer are x and y , respectively. $T(x, y)$ is called *O-rough* if x and y are both odd, *E-rough* if x and y are both even, and *flat* otherwise.

On the other hand, $\{2, 3, \dots, L-1\} \setminus \mathcal{A}$ can also be uniquely partitioned into several maximal closed intervals. They can be viewed as *gaps* in \mathcal{A} . Note that the elements 0, 1 are not taken into consideration because in what follows, we will focus on \mathcal{A} 's which are shifted non-zero difference set of some codeword in an SCAC and thus $0, 1 \notin \mathcal{A}$ by (3). We denote a gap with the smallest integer x and largest integer y by $G(x, y)$. Similar to tubes, we also classify gaps into E-rough, O-rough and flat gaps. Note that it is possible $x = y$ for some gaps but not for tubes of shifted non-zero difference sets.

Assume that \mathcal{C} is an SCAC and \mathcal{I}_j is one of its codewords. We use $T_j(x, y)$ (resp., $G_j(x, y)$) to emphasize a tube (resp., a gap) in the shifted non-zero difference set $d^+(\mathcal{I}_j)$. For example, let $\mathcal{I}_1 = \{0, 4, 7\}$ be one codeword in some code $\mathcal{C} \in \text{SCAC}(26, 3)$. Then $d^+(\mathcal{I}_1) = \{3, 4, 5, 7, 8, 19, 20, 22, 23, 24\}$. There are one O-rough tube $T_1(3, 5)$; two flat tubes $T_1(7, 8)$, $T_1(19, 20)$; and one E-rough tube $T_1(22, 24)$. On the other hand, there are two E-rough gaps $G_1(2, 2)$, $G_1(6, 6)$; one flat gap $G_1(9, 18)$; and two O-rough gaps $G_1(21, 21)$, $G_1(25, 25)$.

Now, we define a special gap, called *solitary* gap, in a code.

Definition 3 Consider a given SCAC, \mathcal{C} , and one of its codewords \mathcal{I}_j . Let $G_j(x, y)$ be a gap in $d^+(\mathcal{I}_j)$ and $T(x', y')$ be a tube in $\bigcup_{\mathcal{I} \in \mathcal{C}} d^+(\mathcal{I})$. If $x \leq x'$ and $y' \leq y$, then this tube is said to be included in the gap, denoted by $T(x', y') \triangleleft G_j(x, y)$. An E-rough (or O-rough) gap $G_j(x, y)$ is said to be *solitary* if there is no E-rough (or O-rough) tube $T(x', y')$ in $\bigcup_{\mathcal{I} \in \mathcal{C}} d^+(\mathcal{I})$ such that $T(x', y') \triangleleft G_j(x, y)$.

For example, let $\mathcal{I}_1 = \{0, 2, 4\}$, $\mathcal{I}_2 = \{0, 6, 12\}$ and $\mathcal{I}_3 = \{0, 9, 19\}$ be the three codewords in a code $\mathcal{C} \in \text{SCAC}(28, 3)$. Then it can be checked that $G_3(2, 8)$ is solitary.

2.2 Previously known results

We summarize some previously known deterministic results on CACs and SCACs of weight three in this subsection.

Theorem 1 ([7]) $M(L, 3) = M^e(L, 3) = (L - 2)/4$ for any $L \equiv 2 \pmod{4}$.

Theorem 2 ([1, 4, 11]) Let $L = 4t$. Then

$$M(L, 3) = \begin{cases} 7L/64 & \text{if } t \equiv 0 \pmod{8}, \\ (7L + 8)/64 & \text{if } t \equiv 1 \pmod{8}, \\ (7L - 48)/64 & \text{if } t \equiv 2, 10 \pmod{24}, \\ (7L + 24)/64 & \text{if } t \equiv 3 \pmod{24}, \\ (7L - 32)/64 & \text{if } t \equiv 4, 20 \pmod{24}, \\ (7L - 24)/64 & \text{if } t \equiv 5, 13 \pmod{24}, \\ (7L - 16)/64 & \text{if } t \equiv 6 \pmod{8}, \\ (7L - 8)/64 & \text{if } t \equiv 7 \pmod{8}, \\ (7L - 40)/64 & \text{if } t \equiv 11, 19 \pmod{24}, \\ (7L + 32)/64 & \text{if } t \equiv 12 \pmod{24}, \\ (7L + 16)/64 & \text{if } t \equiv 18 \pmod{24}, \\ (7L + 40)/64 & \text{if } t \equiv 21 \pmod{24}. \end{cases}$$

Theorem 3 ([18]) The followings hold.

- (i) $M(L, 3) = M^e(L, 3) = (L - 1)/4$ if $L = 2^{2t} + 1$ for $t \geq 1$.
- (ii) $M(L, 3) = M^e(L, 3) = (L + 1)/4$ if $L = 2^{2t} - 1$ for $t \geq 2$.

Theorem 4 ([6]) $M(L, 3) = M^e(L, 3) = (L - 1)/4$ if

- (i) $L = 2^{2t-1} - 2^t + 1$ for $t \geq 2$, or
- (ii) $L = 2^{2t-1} + 2^t + 1$ for $t \geq 1$.

As for SCACs of weight three, there are few results reported in the literature. An exception is the following.

Theorem 5 ([20]) Let L be an integer factorized as $3^q 7^r \ell$, where ℓ is an even integer not divisible by 3 or 7. Then for $L \geq 18$ we have

$$M_S(L, 3) \leq \begin{cases} \lfloor (L - 2)/6 \rfloor & \text{if } q = r = 0, \\ \lfloor L/6 \rfloor & \text{if } q \geq 1, r = 0, \\ \lfloor (L - 1)/6 \rfloor & \text{if } q = 0, r \geq 1, \\ \lfloor (L + 1)/6 \rfloor & \text{if } q \geq 1, r \geq 1. \end{cases}$$

2.3 A Necessary Condition

We close this section with the following necessary condition for the existence of an SCAC. The result delineates the impact of solitary gaps and is based on SCAC characteristics presented in Proposition 1.

Lemma 1 *Consider a given code $\mathcal{C} \in \text{SCAC}(L, \omega)$. If there exists one codeword, say \mathcal{I}_j , having λ solitary gaps in $d^+(\mathcal{I}_j)$, then*

$$L \geq 2 + \lambda + \sum_{\mathcal{I} \in \mathcal{C}} |d^+(\mathcal{I})|.$$

Proof Let $G_j(x, y)$ be one of the λ solitary gaps in $d^+(\mathcal{I}_j)$. We assume that $G_j(x, y)$ is E-rough, i.e., x and y are both even. This implies the number of even integers in $G_j(x, y)$ is one more than that of odd integers. By the definition of the solitary gap, we cannot find an E-rough tube in $\bigcup_{\mathcal{I} \in \mathcal{C}} d^+(\mathcal{I})$, say $T(x', y')$, such that $T(x', y') \triangleleft G_j(x, y)$. From the defining property of flat and O-rough tubes, we know the number of odd integers in a flat or O-rough tube is equal to or bigger than that of even integers. Thus we always can find an even integer in $G_j(x, y)$ which is not included in $\bigcup_{\mathcal{I} \in \mathcal{C}} d^+(\mathcal{I})$. For the case $G_j(x, y)$ is O-rough, the proof goes along the same line as above and is omitted. The result is that there exists an odd integer not included in $\bigcup_{\mathcal{I} \in \mathcal{C}} d^+(\mathcal{I})$.

We conclude that at least λ integers in the interval $[2, L - 1]$ do not belong to $\bigcup_{\mathcal{I} \in \mathcal{C}} d^+(\mathcal{I})$, since there exist λ solitary gaps in $d^+(\mathcal{I}_j)$. Following Proposition 1, we finally obtain that

$$L - 2 - \lambda \geq \left| \bigcup_{\mathcal{I} \in \mathcal{C}} d^+(\mathcal{I}) \right| = \sum_{\mathcal{I} \in \mathcal{C}} |d^+(\mathcal{I})|.$$

□

3 Property of Codewords

Lemma 1 provides a recipe for upper bounding the size of SCAC, which relies on $|d^+(\mathcal{I})|$ for different codewords. In this section, we derive $|d^+(\mathcal{I})|$ for any codeword \mathcal{I} . The following definition is useful for the evaluation of $|d^+(\mathcal{I})|$.

Definition 4 We adopt the terminology in [20] and say that a codeword \mathcal{I} is *dispersive* if any two distinct elements in $d(\mathcal{I})$ are not consecutive. Otherwise, it is *non-dispersive*.

By Proposition 1(i), $|d^+(\mathcal{I})| = 2|d^*(\mathcal{I})|$ if \mathcal{I} is a dispersive codeword in an SCAC.

3.1 Non-equi-difference Codewords

Let $\mathcal{I} = \{0, q_1, q_1 + q_2\}$ be a non-equi-difference codeword in a code $\mathcal{C} \in \text{SCAC}(L, 3)$ for some $q_1, q_2 \geq 2$ and $q_1 + q_2 < L$. After setting $q_3 = L - q_1 - q_2$, we have

$$d^*(\mathcal{I}) = \{q_1, q_2, q_3, L - q_1, L - q_2, L - q_3\}.$$

Now, we write q_1, q_2, q_3 in an ascending order as q_l, q_m, q_u . Since \mathcal{I} is non-equi-difference, q_l, q_m, q_u must be mutually distinct and thus

$$q_l < q_m < q_u, L - q_u < L - q_m < L - q_l. \quad (4)$$

Therefore,

$$|d^*(\mathcal{I})| = \begin{cases} 5 & \text{if } q_u = L/2, \\ 6 & \text{if } q_u \neq L/2. \end{cases} \quad (5)$$

Lemma 2 *Let \mathcal{I} be a non-equi-difference codeword in a code $\mathcal{C} \in \text{SCAC}(L, 3)$ with even L and $d^*(\mathcal{I}) = \{q_l, q_m, q_u, L - q_u, L - q_m, L - q_l\}$, where the three parameters q_l, q_m, q_u satisfy $q_l + q_m + q_u = L$ and the inequality in (4). If $q_u < L/2$, then*

- (i) $|d^+(\mathcal{I})| = 8$ if $q_l + 1 = q_m = q_u - 1 = L/3$; and
- (ii) $|d^+(\mathcal{I})| \geq 10$ otherwise.

Proof By the assumption that $q_u < L/2$, (4) can be written as

$$q_l < q_m < q_u < L - q_u < L - q_m < L - q_l, \quad (6)$$

and thus $|d^*(\mathcal{I})| = 6$. Moreover, $q_l \geq 2$ and $q_u < L/2$ imply respectively that $L - q_l + 1 < L$ and $q_u + 1 < L - q_u$. Then we have

$$d^+(\mathcal{I}) \supseteq d^*(\mathcal{I}) \uplus \{q_u + 1, L - q_l + 1\}.$$

Note that the notation \uplus refers to disjoint union operation, which is used to emphasize that the two involved sets are disjoint.

If $q_l + 1 = q_m = q_u - 1$, then $q_m = L/3$, and $d^+(\mathcal{I})$ is exactly equal to $d^*(\mathcal{I}) \uplus \{q_u + 1, L - q_l + 1\}$. Hence $|d^+(\mathcal{I})| = 8$ in this case.

If $q_l + 1 \neq q_m$, then $q_l + 1$ and $L - q_m + 1$ are included in $d^+(\mathcal{I})$ but not $d^*(\mathcal{I})$. Similarly, if $q_m \neq q_u - 1$, then $q_m + 1$ and $L - q_u + 1$ are in $d^+(\mathcal{I}) \setminus d^*(\mathcal{I})$. In either case, we obtain $|d^+(\mathcal{I})| \geq 10$. This completes the proof. \square

For example, let $L = 24$. If $\mathcal{I} = \{0, 8, 15\}$, then $d^*(\mathcal{I}) = \{7, 8, 9, 15, 16, 17\}$ and $|d^+(\mathcal{I})| = 8$. If $\mathcal{I} = \{0, 6, 13\}$, then $d^*(\mathcal{I}) = \{6, 7, 11, 13, 17, 18\}$ and $|d^+(\mathcal{I})| = 10$.

Lemma 3 *Let \mathcal{I} be a non-equi-difference codeword in a code $\mathcal{C} \in \text{SCAC}(L, 3)$ with even L and $d^*(\mathcal{I}) = \{q_l, q_m, q_u, L - q_u, L - q_m, L - q_l\}$, where the three parameters q_l, q_m, q_u satisfy $q_l + q_m + q_u = L$ and the inequality in (4). If $q_u \geq L/2$, then*

- (i) $|d^+(\mathcal{I})| = 8$ if $q_m = q_l + 1 = (L + 2)/4$, $q_u = L/2$; and
(ii) $|d^+(\mathcal{I})| \geq 10$ otherwise.

Proof We first consider $q_u > L/2$. In this case, (4) can be written as

$$q_l < q_m < L - q_u < q_u < L - q_m < L - q_l.$$

It is easy to see that $L - q_u + 1$ and $L - q_l + 1$ are in $d^+(\mathcal{I}) \setminus d^*(\mathcal{I})$. We now claim that $q_m + 1$ and $q_u + 1$ are also in $d^+(\mathcal{I}) \setminus d^*(\mathcal{I})$. Suppose the assertion is not true; that is, $q_m + 1 = L - q_u$. By the assumption that $q_l + q_m + q_u = L$, we have $q_l = 1$, which contradicts to Proposition 1(i). Therefore,

$$d^+(\mathcal{I}) \supseteq d^*(\mathcal{I}) \uplus \{q_m + 1, L - q_u + 1, q_u + 1, L - q_l + 1\},$$

and thus $|d^+(\mathcal{I})| \geq 10$.

As for the case of $q_u = L/2$, (4) can be written as

$$q_l < q_m < q_u = L - q_u < L - q_m < L - q_l.$$

By the same argument, $q_m + 1, q_u + 1$ and $L - q_l + 1$ are in $d^+(\mathcal{I}) \setminus d^*(\mathcal{I})$. Then we have

$$d^+(\mathcal{I}) \supseteq d^*(\mathcal{I}) \uplus \{q_m + 1, q_u + 1, L - q_l + 1\}.$$

If $q_l + 1 = q_m$, then q_m must be equal to $(L + 2)/4$ and $|d^+(\mathcal{I})| = 8$. If $q_l + 1 < q_m$, then $q_l + 1$ and $L - q_m + 1$ will be in $d^+(\mathcal{I}) \setminus d^*(\mathcal{I})$, and thus $|d^+(\mathcal{I})| \geq 10$. \square

For example, let $L = 26$. If $\mathcal{I} = \{0, 6, 13\}$, then $d^*(\mathcal{I}) = \{6, 7, 13, 19, 20\}$ and $|d^+(\mathcal{I})| = 8$. If $\mathcal{I} = \{0, 5, 13\}$, then $d^*(\mathcal{I}) = \{5, 8, 13, 18, 21\}$ and $|d^+(\mathcal{I})| = 10$.

Proposition 2 *Let \mathcal{I} be a non-equi-difference codeword in a code $\mathcal{C} \in \text{SCAC}(L, 3)$ with even L such that $|d^+(\mathcal{I})| < 10$ and has at least one rough tube. Assume that $d^*(\mathcal{I}) = \{q_l, q_m, q_u, L - q_u, L - q_m, L - q_l\}$, where the three parameters q_l, q_m, q_u satisfy $q_l + q_m + q_u = L$ and the inequality in (4). Then, $q_m = q_l + 1 = (L + 2)/4$, $q_u = L/2$.*

Proof By Lemma 2 and Lemma 3, there are two possible codewords satisfying $|d^+(\mathcal{I})| < 10$. They are the codeword with $q_m = q_l + 1 = q_u - 1 = L/3$ and that with $q_m = q_l + 1 = (L + 2)/4$, $q_u = L/2$, and both have $|d^+(\mathcal{I})| = 8$. By the definition of rough tubes, only the latter one has at least one rough tube. \square

3.2 Equi-difference Codewords

We start this subsection with the following known result on equi-difference codewords.

Lemma 4 ([7]) *Let $\mathcal{C} \in \text{CAC}(L, 3)$ and \mathcal{I} be one of its equi-difference codewords. Then we have*

$$|d^*(\mathcal{I})| = \begin{cases} 2 & \text{if } g = L/3, \\ 3 & \text{if } g = L/4, \\ 4 & \text{otherwise.} \end{cases}$$

Lemma 4 obviously holds for the case of $\mathcal{C} \in \text{SCAC}(L, 3)$ due to $\text{SCAC}(L, 3) \subseteq \text{CAC}(L, 3)$. A codeword \mathcal{I} in a CAC or SCAC of weight three is called *exceptional* [10] if $|d^*(\mathcal{I})| < 4$. Therefore, there are at most two exceptional equi-difference codewords in a CAC or SCAC of weight three.

Lemma 5 ([20]) *Let \mathcal{I} be a non-dispersive equi-difference codeword with generator g in an code in $\text{SCAC}(L, \omega)$. If there are k ($k > 0$) pairs of consecutive elements in $d^*(\mathcal{I})$, then we have*

- (i) $(2w - k - 1)g \equiv \pm 1 \pmod{L}$ with $k \leq w - 1$;
- (ii) g and $2w - k - 1$ are both relatively prime to L ;
- (iii) \mathcal{I} is non-exceptional.

Following Lemma 5 we have:

Corollary 1 *Let \mathcal{I} be a non-dispersive equi-difference codeword with generator g in a code in $\text{SCAC}(L, 3)$ with even L . Then there are two pairs of consecutive elements in $d^*(\mathcal{I})$ and*

$$g = \frac{L+1}{3} \text{ or } \frac{L-1}{3}. \quad (7)$$

Proof Suppose there are k (≥ 1) pairs of consecutive elements in $d^*(\mathcal{I})$. Since L is even and $\omega = 3$, by Lemma 5(i)–(ii), we have $k = 2$, $\gcd(g, L) = 1$ and

$$3g \equiv \pm 1 \pmod{L}.$$

By the assumption that $g \leq L/2$, we have $3g < 2L$, and thus the above equation can be reduced to

$$g = (L+1)/3 \text{ or } (L-1)/3.$$

Note that \mathcal{I} is non-exceptional by Lemma 5 (iii). □

Now we are ready to derive results on $|d^+(\mathcal{I})|$ for a different type of equi-difference \mathcal{I} as follows.

Theorem 6 *Let \mathcal{I} be an equi-difference codeword with generator g in a code in $\text{SCAC}(L, 3)$ with even L . Then we have*

$$|d^+(\mathcal{I})| = \begin{cases} 4 & \text{if } g = \frac{L}{3}, \\ 6 & \text{if } g = \frac{L}{4} \text{ or } \frac{L+1}{3} \text{ or } \frac{L-1}{3}, \\ 8 & \text{otherwise.} \end{cases}$$

Proof Corollary 1 promises that there is only one non-dispersive equi-difference codeword: $g = (L+1)/3$ or $(L-1)/3$. In either case, we always have $|d^+(\mathcal{I})| = 6$.

We now consider that \mathcal{I} is dispersive. It is obvious that $|d^+(\mathcal{I})| = 2|d^*(\mathcal{I})|$. Then the result follows from Lemma 4. \square

As proved in Lemma 2, Lemma 3 and Theorem 6, we conclude that in an SCAC with even length and weight three there are four types of codeword \mathcal{I} satisfying $|d^+(\mathcal{I})| < 8$, each of which is equi-difference. We classify them in Table 1 with notations E_1, E_2, N_1, N_2 , and make an illustration by the following example.

Codeword	Generator	$ d^+(\mathcal{I}) $
\mathcal{I}_{E_1}	$L/4$	6
\mathcal{I}_{E_2}	$L/3$	4
\mathcal{I}_{N_1}	$(L-1)/3$	6
\mathcal{I}_{N_2}	$(L+1)/3$	6

Table 1 The four types of codeword \mathcal{I} with even L and $|d^+(\mathcal{I})| < 8$.

For example, let $L = 28$. Then $\mathcal{I}_1 = \{0, 2, 4\}$, $\mathcal{I}_2 = \{0, 7, 14\}$ and $\mathcal{I}_3 = \{0, 9, 18\}$, the equi-difference codewords generated by 2, 7 and 9 respectively, form a code in $\text{SCAC}(28, 3)$. We have $d^*(\mathcal{I}_1) = \{2, 4, 24, 26\}$, $d^*(\mathcal{I}_2) = \{7, 14, 21\}$ and $d^*(\mathcal{I}_3) = \{9, 10, 18, 19\}$. Notice that $|d^+(\mathcal{I}_2)| = 6$ as the generator $g = 7 = L/4$, and $|d^+(\mathcal{I}_3)| = 6$ as the generator $g = 9 = (L-1)/3$ (i.e., \mathcal{I}_3 is non-dispersive).

4 Upper Bounds on $M_S(L, 3)$

Following the result of $|d^+(\mathcal{I})|$ for different types of codewords in Section 3, we establish upper bounds on $M_S(L, 3)$ under different conditions of L . Since any codeword \mathcal{I} in an SCAC with even length and weight three has $|d^+(\mathcal{I})| \geq 8$ except the four cases listed in Table 1, we first discuss $M_S(L, 3)$ according to the presence of the four codewords: \mathcal{I}_{E_1} , \mathcal{I}_{E_2} , \mathcal{I}_{N_1} and \mathcal{I}_{N_2} . In the following lemma, therefore, L is classified according to its remainder after dividing 12. Note that we only consider $L \geq 18$ in this section as $M_S(L, 3) = 1$ if $L < 18$ (see [20]).

Lemma 6 *Let $L \geq 18$. Then,*

$$M_S(L, 3) \leq \begin{cases} \lfloor (L+4)/8 \rfloor & \text{if } L \equiv 0 \pmod{12}, \\ \lfloor (L+2)/8 \rfloor & \text{if } L \equiv 4, 6, 8 \pmod{12}, \\ \lfloor L/8 \rfloor & \text{if } L \equiv 2, 10 \pmod{12}. \end{cases}$$

Proof Let \mathcal{C} be a code in $\text{SCAC}(L, 3)$ with $|\mathcal{C}| = M = M_S(L, 3)$. Assume that the numbers of codewords $\mathcal{I}_{E_1}, \mathcal{I}_{E_2}, \mathcal{I}_{N_1}, \mathcal{I}_{N_2}$ in \mathcal{C} are e_1, e_2, n_1, n_2 , respectively.

We first consider the case of $L \equiv 0 \pmod{12}$. In this case, $e_1 \leq 1$, $e_2 \leq 1$ and $n_1 = n_2 = 0$ by Table 1. By Proposition 1, we have

$$L \geq 2 + \sum_{\mathcal{I} \in \mathcal{C}} |d^+(\mathcal{I})|. \quad (8)$$

Since $|d^+(\mathcal{I}_{E_1})| = 6$, $|d^+(\mathcal{I}_{E_2})| = 4$, and $|d^+(\mathcal{I})| \geq 8$ if \mathcal{I} is neither \mathcal{I}_{E_1} nor \mathcal{I}_{E_2} , by (8) we have

$$\begin{aligned} L &\geq 2 + 6e_1 + 4e_2 + 8(M - (e_1 + e_2)) \\ &= 2 + 8M - 2e_1 - 4e_2 \\ &\geq 2 + 8M - 2 - 4 = 8M - 4. \end{aligned}$$

Hence $M \leq \lfloor (L+4)/8 \rfloor$.

The other five cases can be dealt with in the same way. Then we complete the proof. \square

In the following lemma, we investigate the case of $L \equiv 12 \pmod{24}$ in more detail.

Lemma 7 *Let $L \geq 18$. If $L \equiv 12 \pmod{24}$, then*

$$M_S(L, 3) \leq (L-4)/8.$$

Proof Similar to the setting in the proof of Lemma 6, let \mathcal{C} be a code in $\text{SCAC}(L, 3)$ with $|\mathcal{C}| = M = M_S(L, 3)$ and assume that the numbers of codewords $\mathcal{I}_{E_1}, \mathcal{I}_{E_2}, \mathcal{I}_{N_1}, \mathcal{I}_{N_2}$ in \mathcal{C} are e_1, e_2, n_1, n_2 , respectively. The conditions $3|L$ and $4|L$ imply that $e_1 \leq 1$, $e_2 \leq 1$ and $n_1 = n_2 = 0$. We aim to show that $L \geq 8M + 4$.

Observe that

$$d^+(\mathcal{I}_{E_1}) = \left\{ \frac{L}{4}, \frac{L}{4} + 1, \frac{L}{2}, \frac{L}{2} + 1, \frac{3L}{4}, \frac{3L}{4} + 1 \right\}.$$

Since $L/4$ is odd, $d^+(\mathcal{I}_{E_1})$ has four rough gaps. Among other possible codewords in \mathcal{C} , only non-equi-difference codewords may have rough tubes. Moreover, if a codeword \mathcal{I} has rough tubes, we have $|d^+(\mathcal{I})| \geq 10$ by Proposition 2 and the assumption that $L \equiv 12 \pmod{24}$.

Assume that there are t non-equi-difference codewords in \mathcal{I} . If $t \geq 1$, then by (8) we have

$$\begin{aligned} L &\geq 2 + \sum_{\mathcal{I} \in \mathcal{C}} |d^+(\mathcal{I})| \\ &\geq 2 + 6e_1 + 4e_2 + 10t + 8(M - (e_1 + e_2 + t)) \\ &= 2 + 8M - 2e_1 - 4e_2 + 2t \\ &\geq 2 + 8M - 2 - 4 + 2 = 8M - 2. \end{aligned}$$

If $t = 0$, otherwise, then the four rough gaps in $d^+(\mathcal{I}_{E_1})$ are all solitary. By plugging $\lambda = 4$ into Lemma 1, we have

$$\begin{aligned} L &\geq 2 + 4 + \sum_{\mathcal{I} \in \mathcal{C}} |d^+(\mathcal{I})| \\ &\geq 2 + 4 + 6e_1 + 4e_2 + 8(M - (e_1 + e_2)) \\ &= 6 + 8M - 2e_1 - 4e_2 \\ &\geq 6 + 8M - 2 - 4 = 8M. \end{aligned}$$

In either case, we obtain $L \geq 8M + 4$ due to $L \equiv 12 \pmod{24}$. \square

We end this section by collecting the results in Lemma 6 and 7.

Theorem 7 *Let $L \geq 18$. Then*

$$M_S(L, 3) \leq \begin{cases} L/8 & \text{if } L \equiv 0 \pmod{8}, \\ (L-4)/8 & \text{if } L \equiv 4 \pmod{8}, \\ (L+2)/8 & \text{if } L \equiv 6 \pmod{24}, \\ (L-2)/8 & \text{if } L \equiv 2, 10, 18 \pmod{24}, \\ (L-6)/8 & \text{if } L \equiv 14, 22 \pmod{24}. \end{cases}$$

5 Optimal SCACs

In this section we will show that the upper bounds of $M_S(L, 3)$ obtained in Theorem 7 are indeed tight in several cases. To construct SCACs attaining these upper bounds, we revisit a construction of SCACs from existing CACs proposed in [20].

Let $\mathcal{C} = \{\mathcal{I}_1, \mathcal{I}_2, \dots, \mathcal{I}_M\}$ be a CAC of length L and weight ω . For $j = 1, 2, \dots, M$ define $2\mathcal{I}_j = \{2t : t \in \mathcal{I}_j\}$. By viewing each $2\mathcal{I}_j$ as an ω -subset of \mathbb{Z}_{2L} , it is obvious that $\{1, 2L-1\} \cap d^*(2\mathcal{I}_j) = \emptyset$ and $d^+(2\mathcal{I}_j) \cap d^+(2\mathcal{I}_k) = \emptyset$ for all $j \neq k$. Thus, $\{2\mathcal{I}_1, 2\mathcal{I}_2, \dots, 2\mathcal{I}_M\}$ forms an SCAC of length $2L$ and weight ω by Proposition 1. Note that the strategy of doubling all elements in \mathcal{I}_j is equivalent to that of padding an extra zero after each entry when considering \mathcal{I}_j as a binary sequence.

Theorem 8 ([20]) *If there exists a CAC of M codewords in $\text{CAC}(L, \omega)$, then there exists an SCAC of M codewords in $\text{SCAC}(2L, \omega)$.*

By Theorem 8, it is easy to see that $M_S(L, \omega) \geq M(L/2, \omega)$ whenever L is even. Therefore, we can obtain several optimal SCACs by Theorem 7, Theorem 8 and some known optimal CACs listed in Section 2.2.

Corollary 2 *Let $L \geq 18$. Then,*

- (i) $M_S(L, 3) = (L - 4)/8$ if $L \equiv 4 \pmod{8}$;
- (ii) $M_S(L, 3) = (L - 2)/8$ if $L = 2^{2t+1} + 2$, $2^{2t} - 2^{t+1} + 2$ or $2^{2t} + 2^{t+1} + 2$ for some t ;
- (iii) $M_S(L, 3) = (L + 2)/8$ if $L = 2^{2t+1} - 2$ for some t .

A bound of $M_S(L, 3)$ for each $L \equiv 0 \pmod{8}$ is also obtained.

Corollary 3 *Let $L = 8t$ for some $t \geq 3$. Then,*

$$\frac{L}{8} \geq M_S(L, 3) \geq \begin{cases} 7L/64 & \text{if } t \equiv 0 \pmod{8}, \\ (7L + 8)/64 & \text{if } t \equiv 1 \pmod{8}, \\ (7L - 48)/64 & \text{if } t \equiv 2, 10 \pmod{24}, \\ (7L + 24)/64 & \text{if } t \equiv 3 \pmod{24}, \\ (7L - 32)/64 & \text{if } t \equiv 4, 20 \pmod{24}, \\ (7L - 24)/64 & \text{if } t \equiv 5, 13 \pmod{24}, \\ (7L - 16)/64 & \text{if } t \equiv 6 \pmod{8}, \\ (7L - 8)/64 & \text{if } t \equiv 7 \pmod{8}, \\ (7L - 40)/64 & \text{if } t \equiv 11, 19 \pmod{24}, \\ (7L + 32)/64 & \text{if } t \equiv 12 \pmod{24}, \\ (7L + 16)/64 & \text{if } t \equiv 18 \pmod{24}, \\ (7L + 40)/64 & \text{if } t \equiv 21 \pmod{24}. \end{cases}$$

In what follows we consider CACs of odd length and weight three. Let $\mathcal{C} \in \text{CAC}(L, 3)$ with odd L and \mathcal{I} be one of its codewords. Since L is odd, we have

$$|d^*(\mathcal{I})| = \begin{cases} 2 & \text{if } \mathcal{I} \text{ is equi-difference with generator } g = \frac{L}{3}, \\ 4 & \text{if } \mathcal{I} \text{ is equi-difference with generator } g \neq \frac{L}{3}, \\ 6 & \text{otherwise.} \end{cases} \quad (9)$$

We say a code $\mathcal{C} \in \text{CAC}(L, 3)$ has *leave* Λ if

$$\mathbb{Z}_L \setminus \bigcup_{\mathcal{I} \in \mathcal{C}} d(\mathcal{I}) = \Lambda.$$

If Λ is empty, then the code \mathcal{C} is said to be *tight*. By (9), we have the following.

Proposition 3 *Let \mathcal{C} be a code in $\text{CAC}^e(L, 3)$ having leave A , where $L \geq 3$ is an odd integer. If $|A| < 4$ and $\{\frac{L}{3}, \frac{2L}{3}\} \not\subset A$, then \mathcal{C} is optimal. Moreover,*

$$|\mathcal{C}| = M^e(L, 3) = M(L, 3).$$

Let $L \geq 3$ be an odd integer and $G(L)$ be a graph with vertex set $V(G) = \{1, 2, \dots, \frac{L-1}{2}\}$ and edge set $E(G)$, defined by $(a, b) \in E(G)$ if $b \equiv \pm 2a \pmod{L}$. Then the graph $G(L)$ is a union of disjoint cycles. Note that a loop is considered as a cycle of length 1, and a pair of multiedges is considered as a cycle of length 2. $G(L)$ is useful in finding the number $M^e(L, 3)$. More precisely, an edge (a, b) in $G(L)$ represents the equi-difference codeword $\{0, a, 2a\}$ in a code of length L , then the number $M^e(L, 3)$ is determined by the size of *maximum matching* in $G(L)$. Let $N_{\text{odd}}(L)$ be the number of odd cycles in $G(L)$. The following equation was given in [2].

$$M^e(L, 3) = \frac{(L-1)/2 - N_{\text{odd}}(L)}{2} + \chi(3|L), \quad (10)$$

where $\chi(A) = 1$ or 0 depends on the statement A is true or false.

For an odd integer $n > 2$ let e_n be the smallest exponent $e \geq 1$ such that $2^e \equiv 1 \pmod{n}$, and let c_n be the smallest exponent $c \geq 1$ such that $2^c \equiv \pm 1 \pmod{n}$. The exponent e_n and c_n are called the *multiplicative order* and the *multiplicative suborder* of 2 modulo n , respectively.

For any odd prime p , Fu et al. [2] characterize the number $N_{\text{odd}}(p)$ in terms of e_p and derive a necessary and sufficient condition for a tight CAC of weight three.

Theorem 9 ([2]) *Let p be an odd prime. Then,*

$$N_{\text{odd}}(p) = \begin{cases} \frac{p-1}{2e_p} & \text{if } p \equiv 7 \pmod{8}, \text{ or } p \equiv 1 \pmod{8} \text{ and } e_p \text{ is odd,} \\ \frac{p-1}{e_p} & \text{if } p \equiv 3 \pmod{8}, \text{ or } p \equiv 1 \pmod{8} \text{ and } 4|(e_p - 2), \\ 0 & \text{if } p \equiv 5 \pmod{8}, \text{ or } p \equiv 1 \pmod{8} \text{ and } 4|e_p. \end{cases}$$

Theorem 10 ([2]) *Let $L = \prod_{i=1}^m p_i^{r_i}$ be an odd integer, where $p_1 < p_2 < \dots < p_m$ are distinct prime factors and each $r_i \in \mathbb{N}$. There exists a tight equi-difference code $\mathcal{C} \in \text{CAC}(L, 3)$ if and only if one of the following holds:*

- (a) $p_1 > 3$ and each p_i satisfies the third condition in Theorem 9; or
- (b) $p_1 = 3, r_1 = 1$, and for $i \geq 2$, p_i satisfies the third condition in Theorem 9.

In $G(L)$, the *standard cycle*, denoted as $\langle 2 \rangle_L$, is the cycle which contains 1. Given a cycle $C = (s_1, s_2, \dots, s_t)$ in $G(L)$ and an integer a . The *modulo product* of C by a , denoted by aC , is the cycle $(a \cdot s_1, a \cdot s_2, \dots, a \cdot s_t) \pmod{L}$ in $G(L)$ where each item takes symmetry with respect to $L/2$; and, the *normal product* of C by a , denoted by $a \times C$, is the cycle $(a \cdot s_1, a \cdot s_2, \dots, a \cdot s_t)$ in $G(aL)$. Two cycles are said to be *congruent*, denoted as \cong , if they have the same length and one of them is a modulo or normal product of the other one. It is easy to see that $C \cong a \times C$. Besides, it is not difficult to see that every cycle in $G(L)$ can be written as $a\langle 2 \rangle_L$ for some integer $1 \leq a < L$. Some properties of $G(L)$ and c_L are given.

Lemma 8 ([2]) *Let L be an odd integer.*

- (1) c_L divides $\varphi(L)/2$.
- (2) *Let $a\langle 2 \rangle_L$ be a cycle in $G(L)$ for some integer a . If $\gcd(a, L) = d$, then $a\langle 2 \rangle_L \cong \langle 2 \rangle_{\frac{L}{d}}$. In particular, $|a\langle 2 \rangle_L| = |\langle 2 \rangle_{\frac{L}{d}}| = c_{\frac{L}{d}}$.*

We now consider equi-difference CACs with small leave set Λ . The main result is as follows.

Theorem 11 *Let $L = \prod_{i=1}^m p_i^{r_i}$ be an odd integer, where $p_1 < p_2 < \dots < p_m$ are distinct prime factors and each $r_i \in \mathbb{N}$. There exists an equi-difference code $C \in \text{CAC}(L, 3)$ with leave Λ of size 2, $\Lambda \neq \{\frac{L}{3}, \frac{2L}{3}\}$, if one of the followings holds:*

- (a) $p_1 > 3$ and each p_i satisfies the third condition in Theorem 9 with exactly one exception, say p_t , which satisfies $c_{p_t} = \frac{p_t-1}{2}$ and $r_t=1$; or
- (b) $p_1 = 3, r_1 = 1$, and for $i \geq 2$, p_i satisfies the third condition in Theorem 9 with exactly one exception, say p_t , which satisfies $c_{p_t} = e_{p_t} = \frac{p_t-1}{2}$ and $r_t=1$.
- (c) $p_1 = 3, r_1 = 2$, and for $i \geq 2$, p_i satisfies the third condition in Theorem 9.

Proof There exists such a code if and only if (i) $N_{\text{odd}}(L) = 1$ and $3 \nmid L$ or (ii) $N_{\text{odd}}(L) = 2$ and $3|L$. In the following we shall prove that conditions (a) implies (i) and conditions (b) and (c) imply (ii).

(a) \Rightarrow (i): Let k be a factor of L . We first claim that c_k is odd if and only if $k = p_t$. It is clear that c_{p_t} is odd. Assume that k is a multiple of some prime factor $p \neq p_t$. Since $2^{e_k} \equiv (\text{mod } k)$ implies $2^{e_k} \equiv (\text{mod } p)$, we have $e_p | e_k$. Suppose to the contrary that c_k is odd. By Lemma 8(2), $\frac{k}{p}\langle 2 \rangle_k \cong \langle 2 \rangle_p$. This implies that c_p is odd, which contradicts to $N_{\text{odd}}(p) = 0$.

Since each cycle in $G(L)$ can be written as the form $a\langle 2 \rangle_L$, where a is an integer in its cycle. Lemma 8(2) says that $a\langle 2 \rangle_L \cong \langle 2 \rangle_{\frac{L}{d}}$ where $d = \gcd(a, L)$, then the length of $a\langle 2 \rangle_L$ is odd only when $a = \frac{L}{p_t}$. Hence, $N_{\text{odd}} = 1$.

(b) \Rightarrow (ii): Let k be a factor of L . Similar to above argument, c_k is even if k is a multiple of some prime factor $p \neq 3, p_t$; and, c_k is odd if $k = 3$ or p_t . Therefore, it suffices to claim that c_{3p_t} is even. We shall prove a stronger property that

$$c_{3p_t} = e_{3p_t} = p_t - 1.$$

Note that $c_n = \frac{e_n}{2}$ if and only if $2^a \equiv -1 \pmod{n}$ for some a . Suppose to the contrary that $c_{3p_t} = \frac{e_{3p_t}}{2}$. Then $2^a \equiv -1 \pmod{3p_t}$ for some a . This implies that $2^a \equiv -1 \pmod{p_t}$ and thus $c_{p_t} = e_{p_t}/2$, a contradiction to the original assumption. So, we have $c_{3p_t} = e_{3p_t}$. In addition, $e_3 | e_{3p_t}$ and $e_{p_t} | e_{3p_t}$ imply that $(p_t - 1) | e_{3p_t}$. By Lemma 8(1), c_{3p_t} divides $\varphi(3p_t)/2$, we have

$$c_{3p_t} = e_{3p_t} = \frac{\varphi(3p_t)}{2} = p_t - 1.$$

This completes the second case.

(c) \Rightarrow (ii): Notice that $\frac{L}{3}\langle 2 \rangle_L$ and $\frac{L}{9}\langle 2 \rangle_L$ are two odd cycles in $G(L)$. Then the result follows from above arguments. \square

A *safe prime* is a prime number p such that $\frac{p-1}{2}$ is also a prime. It is easy to see that $c_p = \frac{p-1}{2}$ if p is a safe prime. Moreover, if $p \equiv 7 \pmod{8}$, then $c_p = e_p = \frac{p-1}{2}$ (by the first condition in Theorem 9). The following result is derived from Proposition 3 and Theorem 11.

Corollary 4 *Let $L > 3$ be an odd integer. Then if $3 \nmid L$ we have*

- (i) $M(L, 3) = M^e(L, 3) = \frac{L-1}{4}$ if $p \equiv 5 \pmod{8}$ for every prime factor p ;
- (ii) $M(L, 3) = M^e(L, 3) = \frac{L-3}{4}$ if there exists exactly one safe prime factor \hat{p} with $\hat{p}^2 \nmid L$ and $p \equiv 5 \pmod{8}$ for any other prime factor p .

If $3|L$ and $9 \nmid L$, then we have

- (iii) $M(L, 3) = M^e(L, 3) = \frac{L+1}{4}$ if $p \equiv 5 \pmod{8}$ for every prime factor p ;
- (iv) $M(L, 3) = M^e(L, 3) = \frac{L-1}{4}$ if there exists exactly one safe prime factor $\hat{p} \equiv 7 \pmod{8}$ with $\hat{p}^2 \nmid L$, and $p \equiv 5 \pmod{8}$ for any other prime factor $p > 3$.

If $9|L$ and $27 \nmid L$, then we have

- (v) $M(L, 3) = M^e(L, 3) = \frac{L-1}{4}$ if $p \equiv 5 \pmod{8}$ for every prime factor $p > 3$.

Remark: Levenshtein and Tonchev [7, Theorem 7] proved that for odd primes L and p , $M(L, 3) = \frac{L-1}{4}$ if $L = 4p+1$ and $M(L, 3) = \frac{L-3}{4}$ if $L = 2p+1$. These two results can be obtained from Corollary 4 (i) and (ii).

By Theorem 7, Theorem 8 and Corollary 4, we have the following results.

Corollary 5 *Let L be an even integer. Then we have*

- (i) $M_S(L, 3) = (L-2)/8$ if $6 \nmid L$ and $L/2$ satisfies the condition of (i) in Corollary 4;
- (ii) $M_S(L, 3) = (L-6)/8$ if $6 \nmid L$ and $L/2$ satisfies the condition of (ii) in Corollary 4;
- (iii) $M_S(L, 3) = (L+2)/8$ if $6|L$, $18 \nmid L$ and $L/2$ satisfies the condition of (iii) in Corollary 4;
- (iv) $M_S(L, 3) = (L-2)/8$ if $6|L$, $18 \nmid L$ and $L/2$ satisfies the condition of (iv) in Corollary 4;
- (v) $M_S(L, 3) = (L-2)/8$ if $18|L$, $54 \nmid L$ and $L/2$ satisfies the condition of (v) in Corollary 4.

6 Conclusion

We establish in Theorem 7 upper bounds on the size of SCAC of even length and weight three, which improve previously known upper bounds in [20]. The new bounds all increase approximately with slope $1/8$ as a function of length L . By constructing SCACs with some optimal CACs, we show the obtained upper bounds are tight in several cases, as stated in Corollary 2 and Corollary 5. In addition, some new optimal CACs are given in Theorem 11.

Acknowledgments The authors would like to express their gratitude to the referees for their helpful comments in improving the presentation of this paper. This work was supported by the Hong Kong RGC Earmarked Grant CUHK414012, the National Natural Science Foundation of China (No. 61301107 and 61174060), the Shenzhen Knowledge Innovation Program JCYJ20130401-172046453 and the Specialized Research Fund for the Doctoral Program of Higher Education of China (No. 20133219120010).

References

1. Fu H.-L., Lin Y.-H., Mishima M.: Optimal conflict-avoiding codes of even length and weight 3, *IEEE Trans. Inform. Theory* **56**(11), 5747–5756 (2010).
2. Fu H.-L., Lo Y.-H., Shum K.W.: Optimal conflict-avoiding codes of odd length and weight three. *Des. Codes Cryptogr.* **72**(2), 289–309 (2014).
3. Gyöfi L., Vajda I.: Construction of protocol sequences for multiple-access collision channel without feedback, *IEEE Trans. Inform. Theory* **39**(5), 1762–1765 (1993).
4. Jimbo M., Mishima M., Janiszewski S., Teymorian A.Y., Tonchev V.D.: On conflict-avoiding codes of length $n = 4m$ for three active users, *IEEE Trans. Inform. Theory* **53**(8), 2732–2742 (2007).
5. Levenshtein V.I.: Conflict-avoiding codes and cyclic triple systems. *Probl. Inf. Transm.* **43**(3), 199–212 (2007).
6. Lin Y., Mishima M., Satoh J., Jimbo M.: Optimal equi-difference conflict-avoiding codes of odd length and weight three. *Finite Fields Appl.* **26**, 49–68 (2014).
7. Levenshtein V.I., Tonchev V.D.: Optimal conflict-avoiding codes for three active users, in *IEEE Int. Symp. Inform. Theory*, Adelaide, Australia, 535–537 (2005).
8. Massey J.L., Mathys P.: The collision channel without feedback, *IEEE Trans. Inform. Theory* **31**(2), 192–204 (1985).
9. Momihara K.: Necessary and sufficient conditions for tight equi-difference conflict-avoiding codes of weight three. *Des. Codes Cryptogr.* **45**(3), 379–390 (2007).
10. Momihara K., Müller M., Satoh J., Jimbo M.: Constant weight conflict-avoiding codes, *SIAM J. Discrete Math.* **21**(4), 959–979 (2007).
11. Mishima M., Fu H.-L., Uruno S.: Optimal conflict-avoiding codes of length $n \equiv 0 \pmod{16}$ and weight 3. *Des. Codes Cryptogr.* **52**, 275–291 (2009).
12. Nguyen Q.A., Gyöfi L., Massey J.L.: Constructions of binary constant-weight cyclic codes and cyclically permutable codes, *IEEE Trans. Inform. Theory* **38**(3), 940–949 (1992).
13. Shum K.W., Chen C.S., Sung C.W., Wong W.S.: Shift-invariant protocol sequences for the collision channel without feedback, *IEEE Trans. Inform. Theory* **55**(7), 3312–3322 (2009).
14. Shum K.W., Wong W.S.: A tight asymptotic bound on the size of constant-weight conflict-avoiding codes. *Des. Codes Cryptogr.* **57**(1), 1–14 (2010).
15. Shum K.W., Wong W.S., Chen C.S.: A general upper bound on the size of constant-weight conflict-avoiding codes. *IEEE Trans. Inform. Theory* **56**(7), 3265–3276 (2010).
16. Shum K.W., Wong W.S.: Construction and applications of CRT sequences, *IEEE Trans. Inform. Theory* **56**(11), 5780–5795 (2010).
17. Wong W.S.: New protocol sequences for random access channels without feedback, *IEEE Trans. Inform. Theory* **53**(6), 2060–2071 (2007).
18. Wu S.-L., Fu H.-L.: Optimal tight equi-difference conflict-avoiding codes of length $n = 2^k \pm 1$ and weight 3. *J. Comb. Des.* **21**, 223–231 (2013).
19. Zhang Y., Shum K.W., Wong W.S.: Completely irrepressible sequences for the asynchronous collision channel without feedback. *IEEE Trans. Vehicular Tech.* **60**(4), 1859–1866 (2011).
20. Zhang Y., Shum K.W., Wong W.S.: Strongly conflict-avoiding codes. *SIAM J. Discrete Math.* **25**(3), 1035–1053 (2011).